802.1X PROTOCOL-BASED MULTICASTING CONTROL METHOD

Field of the Invention

The present invention relates to a multicasting control method in communication networks, in particular to an 802.1X protocol-based multicasting control method.

Background of the Invention

In communications networks, for data forwarding device such as switch or router, it is advantageous for data security and utilization of network resources to forward network data by subscriber groups. For instance, suppose there is a multicasting group G in a communication network, a query message is sent a certain time period after the router forwards the data for said multicasting group G to verify whether any member of said multicasting group G still exists, and members in said multicasting group G sends Internet Group Management Protocol (IGMP) messages again to respond to said query message; in case that no member of said multicasting group exists in the network, the router receives no response, then the router tries to query again, and if the router still receives no message, it deems no member of said multicasting group G exists in the network and then stop forwarding data for said multicasting group G. Due to the fact that data forwarding with said multicasting group management method is more specific when compared to broadcasting mode, data security and forwarding efficiency are higher.

However, traditional LANs using IEEE 802.1x protocol can only implement port-based multicasting control, i.e., add subscribers to multicasting groups through adding ports to those multicasting groups. When a request for joining in a multicasting group is sent from a subscriber's terminal, the network switching device, according to the circumstance, adds the MAC address of said terminal to said multicasting group so as to add the subscriber to said multicasting group. Such a method only provides port number and MAC address of the subscriber's terminal rather than subscriber information, therefore any control related with said subscriber can't be performed due to lack of subscriber information. Though IEEE802.1X protocol is a port-based network access control protocol, which supports subscriber management and accepts multi-subscriber authentication through a single port, such capability can't be utilized to control addition of subscribers to a multicasting group, resulting in

uncontrollability of addition of subscribers to a multicasting group.

Summary of the Invention

It is the object of the present invention to provide an 802.1X protocol-based multicasting control method to implement controllability of addition of subscriber to multicasting group.

To attain the above object, an 802.1X protocol-based multicasting control method, comprising the following steps:

Step 1: intercepting the request message for joining in a multicasting group sent by an authenticated subscriber;

Step 2: obtaining the port and MAC address of the subscriber from the intercepted message;

Step 3: searching corresponding subscriber account information from the authenticated data according to said port and MAC address;

Step 4: authenticating the subscriber's account number and multicasting IP address, and then adding the subscriber to the multicasting group if the authentication is passed successfully; otherwise the subscriber's request is rejected.

Said method further comprises: the authentication server at 802.1X authentication end is utilized to authenticate the subscriber's account number and multicasting IP address.

The authentications of subscriber's account number and multicasting IP address are implemented through verifying whether the multicasting IP address is authorized to accept the subscriber with said account number.

If said 802.1X is based on port authentication, when a subscriber attached to said port makes a request for joining in a multicasting group, the subscriber's MAC address is searched for first; if said MAC address is found, the subscriber's account number is searched for according to said MAC address and port number;

if said 802.1X protocol is based on MAC authentication, when a subscriber attached to said port makes a request for joining in a multicasting group, the subscriber's account number is searched for directly according to the subscriber's MAC address and port number.

The subscriber joins in the multicasting group through IGMP protocol.

According to the method of the present invention, when a subscriber authenticated through 802.1X protocol requests to join in a multicasting group, the request message for joining in the

multicasting group is intercepted first, and then the subscriber's port and MAC address information is obtained from said intercepted message instead of adding the subscriber directly to the multicasting group, then corresponding subscriber information is searched for from authenticated data according to said port and MAC address information, and the subscriber's account number and multicasting IP address are authenticated again, and then the subscriber is added to the multicasting group if the authentication is passed successfully, otherwise the subscriber's request is rejected. Said solution can implement controlled multicasting, authentication of the legality of adding to multicasting, and accounting; in addition, said method doesn't require modification to multicasting client software or server software, instead, only simple configuration at 802.1X device end and authentication server at authentication end is necessary, it is advantageous for protection of existing investment and compatibility to existing software.

Brief description of the Drawings

Fig. 1 shows the architecture of 802.1X protocol;

Fig.2 shows the architecture of 802.1X authentication-based controlled multicasting;

Fig.3 shows the authentication process of 802.1X authentication-based controlled multicasting;

Fig.4 is the flow chart of an embodiment of the method according to the present invention.

Detailed description of the Embodiment

The present invention is described in further detail hereunder with reference to the drawings.

Referring to Fig.1, wherein the IEEE802.1X protocol shown in Fig.1 is a port-based network access control protocol and is used to authenticate and control client access at physical layer of network devices. There are three entities in Fig.1: 802.1X client end, 802.1X device end, and authentication end. Authentication information is exchanged through extensible authentication protocol (EAP) between authentication servers of authentication end and 802.1X device end. EAPOL serves as the authentication protocol between 802.1X client end and 802.1X device end. Usually, 802.1X device end is implemented at access layer of network; 802.1X client end is installed in subscriber's PC; 802.1X authentication server system usually resides in the operator's

AAA (Accounting, Authentication, and Authorization) center. There are controlled ports and uncontrolled ports inside of 802.1X device end. The uncontrolled ports are always in two-way connected state and are mainly used to transfer EAPOL frames; therefore, EAPOL frames can be received and sent via the uncontrolled ports at any time. The controlled ports are opened only when the authentication is passed so as to transfer network resources and services. According to the application environment, the controlled ports may be configured as two-way controlled or one-way controlled. With above architecture, if the 802.1X device end is implemented with an Ethernet switch or broadband access device, any subscriber device of client end connected to ports on the Ethernet switch or broadband access device can access internal network resources if it passed the authentication; otherwise it can't access internal network resources. Above ports may be physical ones or logical ones, for instance, a typical application is to connect a client PC to a physical port of the Ethernet switch.

Currently, Radius protocol can also run between 802.1X device end and authentication server in the architecture shown in Fig.1; so the authentication server is a Radius server, and the 802.1X device end may be deemed as a client connected to the Radius server.

Seen from above, in the architecture shown in Fig.1, 802.1X protocol will be triggered to authenticate the subscriber when the Ethernet switch transfers the EAPOL-Start message sent from an 802.1X client end to the 802.1X device end. After the authentication server at authentication end successfully authenticate the subscriber, controlled ports of 802.1X device end are opened to transfer network resources and services for the subscriber. Hence the subscriber is online. If the host of a subscriber online wants to add to a multicasting group, said host sends an IGMP message (suppose IGMP protocol is used, in fact, it is not limited to the protocol) to the Ethernet switch (device end) through multicasting client software to indicate to join in said multicasting group, thus the Ethernet switch begins to forward the data of said multicasting group to said subscriber's host.

As the result, network connection to the subscriber will be established through 802.1X protocol as long as the subscriber passes 802.1X protocol-based authentication. On that basis, if the subscriber requests to join in a multicasting group, the MAC address and port number of the subscriber's host may be obtained from the subscriber's message or request transferred through the connection. In this way, detailed information of the subscriber

can be obtained from the subscriber's authentication data according to said MAC address and port number so as to implement control of multicasting addition and to solve uncontrollability issue of multicasting addition according to traditional methods.

The basic principle of the present invention is shown in Fig.2. The Ethernet switch shown in Fig.2 is designed to connect the client end shown in Fig.1 and implement the device end shown in Fig.1. Therefore, said Ethernet switch is used to control switch on/off of network connection to the client. Because that the ports on the Ethernet switch are unavailable for unauthenticated subscribers but can be configured automatically and dynamically and can be used to access network resources for authenticated subscribers, the 802.1X protocol-based Ethernet switch shown in Fig.2 brings operation features to operators. The Ethernet switch as 802.1X device end in Fig.2 employs a Radius protocol module to transfer authentication information to the Radius server as authentication end. The 802.1X authentication module is used to receive 802.1X protocol-based authentication information sent by the subscriber from the corresponding port on the Ethernet switch and transfers said authentication information (containing detailed information of the subscriber, such as user name and password, etc) to the authentication server at the authentication end for authentication through the Radius authentication module. If the subscriber passes the authentication, the authenticated information contains detailed information of the subscriber, and the 802.1X authentication module will launch a port service channel (equivalent to connecting to the switch K1 in Fig.2) for the subscriber. In this way, the subscriber may access network resources through that port service channel, i.e., an 802.1X protocol-based network connection is established for the subscriber. On the basis of above 802.1X connection, if the subscriber sends a request message (suppose it is an IGMP-based message) to join in a multicasting group through said port service channel, the multicasting control module in the Ethernet switch can be configured to intercept said IGMP message so as to obtain the subscriber's MAC address and port number in the IGMP message, and then obtains the subscriber's account number information (user name, password, etc.) through the 802.1X connection for the subscriber according to said MAC address and port number, next, a controlled multicasting connection is established according to the subscriber's information and the multicasting IP address, i.e., the multicasting control module controls the switch on/off of the multicasting switch K2 as required. Therefore the combination of multicasting and 802.1X authenticated port and

subscriber's MAC address delivers controllability of multicasting addition. As for the case in Fig.2, the 802.1X authentication module controls switch K1 of the port service channel, and the multicasting control module controls the multicasting switch K2 of the port service channel.

Fig.4 is the flow chart of an embodiment of the method according to the present invention. Please refer to Fig.3 for the 802.1X authentication-based controlled multicasting authentication process described in Fig.4. It is noted that the embodiment shown in Fig.4 supposes IGMP protocol is used to add the subscriber to the multicasting group and the multicasting control module in the Ethernet switch is preconfigured to intercept the IGMP message sent by the subscriber. As shown in Fig.4, in step 1, the subscriber sends an EAPOL message to trigger 802.1X protocol authentication at 802.1X device end at the beginning of online, i.e., the EAPOL message is transferred to the 802.1X authentication module in the Ethernet switch (device end); in step 2, the 802.1X authentication module sends the subscriber's authentication information to the Radius server at authentication end for authentication via the Radius module. When the authentication is passed successfully, the authenticated subscriber information is stored in the Ethernet switch (e.g. in the 802.1X authentication module). Said two steps are mainly designed to accomplish subscriber authentication process and bring the subscriber online. If the authenticated subscriber sends an IGMP message in step 3 to request to join in a multicasting group, the multicasting control module intercepts the IGMP message in step 4; here, the multicasting control module will not add that subscriber to the multicasting group directly, instead, it sends the subscriber's port number and MAC address information obtained from the IGMP message to the 802.1X authentication module, which searches for corresponding subscriber account number information in the authenticated data according to port and MAC address information, and then feeds back said subscriber account information to the multicasting control module; in step 6, the multicasting control module sends the subscriber's account number and multicasting IP address to the Radius server at authentication end for authentication via the Radius module again, i.e., the Radius server authenticates the subscriber according to the subscriber's account number and multicasting IP address through verifying whether said multicasting IP address is authorized to accept the subscriber of said account number; if the authentication is passed successfully, the subscriber is added to said multicasting group in step 7; otherwise the subscriber's request is rejected. After

the subscriber is added to said multicasting group, the multicasting control module maintains said multicasting connection till the subscriber request exits.

It should be noted that because the 802.1X protocol-based authentication on existing Ethernet switches may be port-based or MAC address-based, the two cases should be treated differently. In port-based authentication mode, the 802.1X module for each port only controls a single authenticated subscriber and hence only maintains one 802.1X connection; however, when the 802.1 authentication is passed, said port can be attached with several client PCs. As a result, when any of the client PCs attached to that port requests to join in a multicasting group, the MAC substitution method is used, i.e., the Ethernet switch will instruct the 802.1X module to verify whether the subscriber's MAC address exists; if yes, it indicates the subscriber has passed the authentication, the 802.1X module will return the authenticated subscriber's MAC address to the Ethernet switch. The multicasting control module then searches for the subscriber's account number according to the returned MAC address and port number.

In MAC address-based authentication mode, the 802.1X module has authenticated each PCs attached to the port and corresponding connections are available. Therefore, when a subscriber attached to said port requests to join in a multicasting group, the Ethernet switch will query the subscriber's MAC address directly in the 802.1X module; when the 802.1X module returns the MAC address, the Ethernet switch will search for the subscriber's account number according to the MAC address and port number. Therefore, each subscriber can find corresponding 802.1X connection according to respective MAC address and port number, i.e., the subscriber's account information can be obtained.

The embodiment shown in Fig.4 employs a Radius server to manage the subscribers' information. Therefore, the embodiment also employs the Radius server to control the addition of subscriber multicasting. In detail, it is implemented through adding a controlled multicasting property item in the Radius server, i.e., the subscriber's account number is configured on the Radius server, and then the value-added multicasting service is added to said account number. With that property item, one or more multicasting addresses can be added for the subscriber. When the Radius server receives an authentication request containing the subscriber's account number and multicasting IP address, if the controlled multicasting property is available, the Radius server will verify whether the multicasting IP address is authorized; if it is

authorized, the Radius server returns an "authentication passed" message, otherwise the Radius server returns an "authentication failed" message.

As a result, the multicasting service property item can be attached to the subscriber's account as a value-added service property, i.e., the subscriber is added first, and then a multicasting channel is launched for said subscriber. In this way, the value-added multicasting service may be implemented for operators according to the present invention to separate value-added multicasting service accounting from elementary 802.1X access authentication connection accounting, in order to facilitate settlement between different service providers.